VENABLE LLP

the download

DEVELOPMENTS IN E-COMMERCE, PRIVACY, INTERNET ADVERTISING, MARKETING AND INFORMATION SERVICES LAW AND POLICY

ISSUE EDITORS

Stuart P. Ingis
singis@Venable.com
202.344.4613

Michael A. Signorelli
masignorelli@Venable.com
202.344.8050

Ariel S. Wolf
awolf@Venable.com
202.344.4464

ADDITIONAL CONTRIBUTORS

Emilio W. Cividanes
ecividanes@Venable.com
202.344.4414

Julia Kernochan Tama
jktama@Venable.com
202.344.4738

Kelly A. DeMarchis
kademarchis@Venable.com
202.344.4722

Tara Sugiyama Potashnik
tspotashnik@Venable.com
202.344.4363

Robert Hartwell
rhartwell@Venable.com
202.344.4663

www.Venable.com

June 2014

In this Issue:

Heard on the Hill

Senate Judiciary Subcommittee Holds Hearing on the Location Privacy Protection Act

On June 4, 2014, the Senate Judiciary Committee's Subcommittee on Privacy, Technology and the Law held a hearing to consider S. 2171, the Location Privacy Protection Act as introduced by the Subcommittee Chairman, Senator Al Franken (D-MN).

S. 2171 would prohibit the development, sale, and use of "stalking apps," which Senator Franken described as mobile applications that secretly track individuals and are often used to commit acts of domestic violence. The bill would also place new restrictions on the commercial collection of location data from mobile devices.

Senator Franken and Senator Jeff Flake (R-AZ) were the primary senators at the hearing. Both senators voiced support for the anti-stalking provisions of the bill. However, Senator Flake stated that he had concerns about the commercial restrictions in the bill harming innovation.

The first witness panel consisted of representatives from the federal government, including the Federal Trade Commission (FTC) and the Department of Justice. The panel also expressed support for the anti-stalking provisions of the bill. The FTC representative requested that the commercial provisions of the bill include enforcement authority for the Commission. The panel also criticized current disclosures regarding location data collection by commercial entities.

The second panel consisted of industry representatives, including the Digital Advertising Alliance (DAA), as well as consumer advocates. This panel discussed current industry efforts to self-regulate data collection and sharing, as well as how these activities may impact the economy.

Senate Permanent Subcommittee on Investigations' Hearing and Report on Potential Security threats in Online Advertising

On May 15, 2014, the U.S. Senate Homeland Security and Governmental Affairs Committee's Permanent Subcommittee on Investigations (PSI) held a hearing with industry stakeholders and a representative of the Federal Trade Commission (FTC) to examine potential security threats that Internet users may face from online advertising, specifically the potential for cybercriminals to use online advertising to deliver malicious software. During the hearing, Senator John McCain (R-AZ), Ranking Member of the PSI, discussed findings and recommendations from a related PSI report released a day before the hearing.[1] At the hearing, Senator McCain announced that in light of potential security threats in online advertising, he is considering reintroducing the Commercial Privacy Bill of Rights Act, a bill that he co-introduced with former Senator John Kerry in the previous session of Congress.

The PSI report focuses on the potential threat of "malvertising," defined as "advertisement-based malware,"[2] and includes recommendations for advertisers and self-regulatory groups to take action to address such security threats. The report recommends that the industry: (1) establish better practices and clearer rules to prevent online advertising abuses; (2) strengthen security information exchanges within the online advertising industry to prevent abuses; (3) clarify specific prohibited practices in online advertising to prevent abuses and protect consumers; and (4) develop additional "circuit breakers" to protect consumers.

---

[1] U.S. Senate Homeland Security and Governmental Affairs Committee Permanent Subcommittee on Investigations, Online Advertising and Hidden Hazards to Consumer Security and Data Privacy (May 14, 2014), *available at* http://www.hsgac.senate.gov/download/?id=3B38A382-8E10-4527-904C-24F37A0D6220 ("Report").

[2] Report at 1.

During the hearing, Senators McCain and Carl Levin (D-MI), Chairman of PSI, questioned industry stakeholders on how they plan to address potential consumer concerns regarding malvertising. Representatives of tech companies testifying at the hearing described the data security protocols and technologies their companies have in place to help address the issue, such as robust scanning to detect malware. Lou Mastria, Executive Director of the Digital Advertising Alliance (DAA), discussed how the DAA's Self-Regulatory Principles offer consumers transparency and choice to control the collection and use of web viewing data by third parties for advertising purposes. Maneesha Mithal, Associate Director of the FTC's Division of Privacy and Identity Protection, explained the FTC's concerns regarding malvertising and noted that the FTC encourages industry self-regulation in online advertising.

From the White House

White House Issues Big Data Report

On May 1, 2014, the White House released its report, "Big Data: Seizing Opportunities, Preserving Values" (Big Data Report). The Big Data Report compiles and analyzes findings from workshops and meetings that were intended to address what makes "big data" unique, the interplay of big data and privacy, and how existing policies and the Consumer Privacy Bill of Rights may apply to big data. The Big Data Report includes six policy recommendations: (1) advance the Consumer Privacy Bill of Rights; (2) pass national data breach legislation; (3) extend privacy protections to foreign individuals; (4) ensure that student data is collected only for educational purposes; (5) increase technical education to reduce discrimination; and (6) amend the Electronic Communications Privacy Act.

The Big Data Report comes after a ninety-day scoping exercise requested by President Obama in January. For this exercise, White House advisor John Podesta led a working group on big data composed of senior government officials. The working group held three workshops and consulted with representatives of industry, academia, civil rights groups, law enforcement, and government agencies.

The President's Council of Advisors on Science & Technology also issued a report on the same day entitled "Big Data and Privacy: A Technological Perspective," which analyzes the technologies used in big data analysis.

White House Calls on the Department of Commerce to Draft Privacy Bill

In the White House Big Data Report issued on May 1, 2014, the White House called on the Department of Commerce (Department) to seek public comment on how the Consumer Privacy Bill of Rights—a proposal for legislation articulated by the Obama Administration in its Privacy Report of February 2012—could support the innovations of big data while at the same time responding to its risks. The Report also asked the Department to seek comment on how the Consumer Privacy Bill of Rights could encompass the responsible use framework described in the Big Data Report.

Accordingly, the Department published its Request for Public Comment in the Federal Register on June 6, 2014, with a period of 60 days available for the public to submit comments.[3] The Request for Comment invites public comment from all stakeholders, including the commercial, academic, and public interest sectors; legislators; and governmental consumer protection and enforcement agencies. Following the comment period, the White House report called on the Department of Commerce to write draft legislation to be considered by stakeholders and ultimately for the President to submit to Congress.

Around the Agencies

Federal Trade Commission Reports on "Data Brokers"

The Federal Trade Commission (FTC) released a study entitled "Data Brokers: A Call for Transparency and Accountability" on May 27, 2014 (Report).[4] The Report is based on the FTC's 2012 request for information issued to nine companies the FTC views as "data brokers," a term the FTC defines to include "companies that collect consumers' personal information and resell or share that information with others."[5] The Report focuses on practices that fall outside the Fair Credit Reporting Act, and can be grouped into three categories: (1) marketing, (2) risk mitigation, and (3) people search.

In the Report, the FTC recommends that Congress consider legislation to give consumers more transparency and data access

---

[3] Big Data and Consumer Privacy in the Internet Economy, 79 Fed. Reg. 32715 (Jun. 6, 2014), *available at* http://www.ntia.doc.gov/files/ntia/publications/big_data_rfc.pdf

[4] Federal Trade Commission, "Data Brokers: A Call for Transparency and Accountability" (May 2014), *available at* http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[5] *Id.* at i.

for products in each of these three categories. In addition, the Report calls upon the industry to implement a "privacy by design" approach, to strengthen measures to avoid collecting data from children and teenagers for marketing and other purposes, and to take reasonable precautions to ensure that downstream recipients are not using data for eligibility determinations or illegal discrimination.

NTIA Multistakeholder Process Continues

On June 3, 2014, the National Telecommunications and Information Administration (NTIA) convened its seventh "Privacy Multistakeholder Meeting" on developing a code of conduct for facial recognition technology (FRT). While the first several meetings explored FRT technology and current and prospective applications, this meeting continued a shift away from fact-finding and toward a discussion about developing a code of conduct. In this context, participants of the meeting focused on elements that would need to be addressed in a code of conduct, such as which entities are covered, and issues of scope and consent.

The stakeholders discussed potential issues involving "facial profiling," described as the use of FRT to tag characteristics (e.g., names, ethnicity, or gender) to facial templates. Participants agreed to examine facial profiling further during the process of drafting a code of conduct. The group also considered issues surrounding the timing of offering and obtaining consent for the use of FRT. In examining these issues, participants discussed use cases such as a casino identifying card-counters through video surveillance. The group also considered, but did not resolve, whether "personally identifiable information" (PII) under the Privacy Act of 1974 should be used as guidance for obligations in a code of conduct for FRT.

On June 24, 2014, NTIA convened the eighth meeting to discuss potential risks and issues associated with FRT and definitions that would be included in a code of conduct. Participants also discussed a draft proposal containing recommendations for commercial use of biometric technology.

Regarding the proposal, the discussion focused on the distinction made between PII and biometric data, as well as between anonymity and privacy. The group discussed a document containing draft definitions of terms for a code of conduct, and began to enumerate potential risks that could be addressed in a code of conduct, including issues arising from storage of facial templates, data breaches, withdrawal of templates from a database, and government access. The next meeting is expected to take place in July.

Consumer Financial Protection Bureau Takes Action on Privacy Issues

The Consumer Financial Protection Bureau (CFPB) recently took two regulatory steps related to financial privacy. In May, the CFPB released a proposal to amend its annual privacy notice requirement under the Gramm-Leach-Bliley Act (implemented through Regulation P). Dozens of public comments were filed on the proposal before the June 12, 2014 deadline. Currently, "financial institutions" subject to Regulation P must provide their customers with initial and annual notices regarding their privacy policies via mail. The CFPB has proposed to allow financial institutions that do not engage in certain types of information-sharing activities to stop mailing an annual disclosure if they post the annual notices on their websites and meet certain other conditions, including using the model notice form set out in Regulation P. This new approach responds to public comments the CFPB previously received on the topic of streamlining regulations the CFPB inherited from other agencies.

Additionally, in conjunction with a field hearing held on June 12, 2014 in New Orleans, the CFPB released a request for information on mobile financial products, and particularly on opportunities for serving economically vulnerable consumers. Comments responding to this request are due on September 10, 2014. Among other issues, the CFPB has requested information on privacy and security concerns that may be associated with mobile financial services, data breach potential, and possible risks associated with creating marketing segments associated with mobile financial customers.

Federal Trade Commission Concludes Spring Privacy Seminar

In May 2014, the Federal Trade Commission (FTC or Commission) concluded its spring privacy series with a seminar on "Consumer Generated and Controlled Health Data." Opening remarks were delivered by Commissioner Julie Brill, who asserted that more consumer protections are needed around health data. The day's seminar also included two presentations, on health data flows and data sharing by popular health and fitness apps, and a panel discussion. The panel discussion featured four panelists from the government and private sector who focused on the distinctions between the types of information and entities covered by the Health Insurance Portability and Accountability Act (HIPAA) and those that are not covered by HIPAA.

This seminar was the Commission's third and final installment in its 2014 Spring Privacy Series. Earlier seminars included presentations and panel discussions on Mobile Device Tracking and Alternative Scoring products. The March 19th seminar, focusing on alternative scoring and predictive analytics, featured a presentation on creating predictive analytics and the benefits of various types of predictive models, including fraud prevention, recommendation engines, and spam filtering. A panel discussion

also featured six panelists from industry, government, and the consumer advocate community, focusing on the application of existing laws to predictive analytics and the accuracy of predictive models.

The mobile device tracking seminar, held earlier in the year, followed a similar format of presentation and panel discussion. Its focus was on the types of information gathered by mobile devices, data retention policies, and privacy considerations. The presentations demonstrated different technologies used to facilitate the collection of users' information from mobile devices and presented research findings into consumers' awareness of these technologies.

In the States

California Attorney General Issues Privacy Policy Guidance

On May 21, 2014, the California Attorney General's Office (CA AG) issued guidance regarding online privacy policies entitled Making Your Privacy Practices Public: Recommendations on Developing a Meaningful Privacy Policy (Guidance). The Guidance offers suggestions for website operators to take into account when drafting privacy policies in compliance with California's Online Privacy Protection Act (CalOPPA). The Guidance offers recommendations on ten aspects of privacy policies, but states that it does not represent new regulations, mandates, or legal opinions. These aspects are:

- Scope of the Policy;
- Availability;
- Readability;
- Data Collection;
- Online Tracking/Do Not Track (DNT);
- Data Use and Sharing;
- Individual Choice and Access;
- Security Safeguards;
- Effective Data; and
- Accountability.

While the Guidance offers recommendations on all aspects of privacy policies, a primary focus is placed on how to comply with the new DNT provisions. While not binding, the Guidance recommends that website operators disclose clearly how they respond to DNT signals, and how the website may use information collected through online tracking. The Guidance also suggests that website operators that comply with CalOPPA by posting links to third-party DNT programs or protocols should disclose if the website participates in such programs and should check if the linked page discloses how a choice may be made regarding online tracking.

About Venable's Privacy and Data Security Team

Venable's privacy and data security attorneys, pioneers in the field, provide an integrated approach to legal and business solutions in e-commerce, Internet advertising, financial services, homeland security and government surveillance, telemarketing and medical privacy. Our attorneys are well-versed in the evolving U.S., Canadian, European and Asian regulations governing our clients' businesses, and assist with drafting statutes and regulations. Our clients represent a variety of industries and are supported by Venable's renowned Legislative and Government Affairs, Advertising, IP and Communications Practices. Venable's Privacy and Data Security Practice is recognized in Chambers Global and the U.S. Legal 500 and has won the Chambers USA Award for Excellence.

About Venable

An American Lawyer Global 100 law firm, Venable serves corporate, institutional, governmental, nonprofit and individual clients throughout the U.S. and around the world. Headquartered in Washington, DC, with offices in California, Maryland, New York and Virginia, Venable LLP lawyers and legislative advisors serve the needs of our domestic and global clients in all areas of corporate and business law, complex litigation, intellectual property, regulatory, and government affairs.

Venable's Privacy and Data Security Team serves clients from these office locations:

WASHINGTON, DC
575 7TH STREET NW
WASHINGTON, DC 20004
t 202.344.4000
f 202.344.8300

NEW YORK, NY
ROCKEFELLER CENTER
1270 AVENUE OF THE AMERICAS
25TH FLOOR
NEW YORK, NY 10020
t 212.307.5500
f 212.307.5598

SAN FRANCISCO, CA
SPEAR TOWER, 40TH FLOOR
1 MARKET STREET
SAN FRANCISCO, CA 94105
t 415.653.3750
f 415.653.3755

LOS ANGELES, CA
2049 CENTURY PARK EAST
SUITE 2100
LOS ANGELES, CA 90067
t 310.229.9900
f 310.229.9901

BALTIMORE, MD
750 E. PRATT STREET
SUITE 900
BALTIMORE, MD 21202
t 410.244.7400
f 410.244.7742

TYSONS CORNER, VA
8010 TOWERS CRESCENT DRIVE
SUITE 300
VIENNA, VA 22182
t 703.760.1600
f 703.821.8949